UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/576,250	04/18/2006	Stefano Brusotti	09952.0027-00000	8838

22852   7590   10/26/2010
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
PHAM, LUU T

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/26/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

<table>
<tr><td rowspan="2">Office Action Summary</td><td>Application No.
10/576,250</td><td>Applicant(s)
BRUSOTTI ET AL.</td></tr>
<tr><td>Examiner
LUU PHAM</td><td>Art Unit
2437</td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _04 August 2010_.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _37-72_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _37-72_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application

is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37

CFR 1.17(e) has been timely paid, the finality of the previous Office action has been

withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/04/2010 has

been entered.

2.   Claims 1-72 have been examined and are pending. **This Action is made Non-FINAL**.

Response to Arguments

3.   The rejection of claim 72 under 35 U.S.C. § 101 is withdrawn as the claim has been

amended.

4.   Applicants' arguments in the instant Amendment, filed on 08/04/2010, with respect to

limitation listed below, have been fully considered but they are not persuasive.

Applicants' arguments:

Baehr does not disclose or suggest *"in the absence of an adverse effect, allowing, by*

said test system, the communication entities not having the adverse effect to

communicate with said set of machines."

The Examiner disagrees for the following reasons:

Baehr does disclose in the absence of an adverse effect, allowing, by said test system, the communication entities not having the adverse effect to communicate with said set of machines *(col. 7, lines 39-43; another action can, of course, be to simply pass the packet through to its destination [targeted hosts/servers]; col. 10, lines 27-32; if the connection is not allowed, it is blocked (box 970), but otherwise, it is allowed, and then the method tests whether it is an initial connection (box 980) - if so, then at box 990 the connection is established [allowing communication between public network and private network i.e., targeted hosts/servers]).* The Examiner respectfully suggests that the claim be further amended to distinguish the claimed invention over prior art of record.

5. Applicant's arguments with respect to limitation *"running said communication entities directed toward said test system on said test facilities to detect possibly adverse affects on said test system"* have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

7.   This application currently names joint inventors. In considering patentability of the claims

under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various

claims was commonly owned at the time any inventions covered therein were made absent

any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to

point out the inventor and invention dates of each claim that was not commonly owned at

the time a later invention was made in order for the examiner to consider the applicability

of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C.

103(a).

8.   **Claims 37-39, 46-51, 54-56, 63-68, and 71-72 are rejected under 35 U.S.C. 103(a)** as

being unpatentable over Baehr et al., (hereinafter "Baehr"), U.S. Patent No. 5,878,231,

issued on March 02, 1999, in view of Nakae et al., (hereinafter "Nakae"), U.S. Patent

Application Publication No. 2004/0172557, filed on August 20, 2003.

- **Regarding claim 37**, Baehr discloses a method of preventing intrusion in

communication traffic with a set of machines in a network, said traffic comprising

communication entities *(col. 5, lines 7-11; Figs. 6-7; proxy network 445 implemented on*

screening system 340), comprising the steps of:

   providing a test system *(col. 5, lines 7-11; Fig. 7; the screen 340 and proxy*

network in a single unit [as a whole, known as test system]) comprising test facilities

replicating at least one of said machines in said set *(col. 4, lines 27-40 and lines 50-63;*

Figs. 5-6; proxy network may include proxy hosts representing actual hosts, and/or proxy

hosts with unique server; proxy network 430/445 includes a virtual host mirroring (or

acting as proxy for) each of a subset (or all) of the hosts found on the private network 330;

col. 5, lines 7-11; Fig. 7; the proxy hosts 360-380 are emulated by the program

instructions, so that all of the behavior of any of the actual hosts may be mimicked by a

virtual proxy host module);

   directing at least part of said communication entities in said traffic toward said

test system *(col. 2, lines 25-36; if the packet's intended destination is a host machine on the*

private network, it may instated be sent aside to a preconfigured host machine on the proxy

network, which executes appropriate operations that the actual host would execute; col. 4,

lines 57-60; Figs. 4-7; when a user attempts to access a service or host of the private

network, the request may be shunted aside to the proxy network to either a mirroring proxy

host or a unique proxy host; see also col. 6, lines 30-36; see also col. 10, lines 11-34);

   running said communication entities directed toward said test system [[on said

test facilities]] to detect possibly adverse affects on said test system *(col. 6, lines 30-50;*

col. 8, lines 67 to col. 9, lines 1-7; col. 9, liens 26-35; packet inspector 600 includes the

instructions for inspecting the contents of the incoming packets based upon the criteria

discussed above); and

       i) in the presence of an adverse effect, blocking, by said test system, the

communication entities leading to said adverse effect *(col. 6, lines 53-59; this is an*

indication that intruder may be attempting to breach the private network by masquerading

as a trusted hot; in this case, the screen 340 should drop the packet without reply; col. 7,

lines 16-24; packets from any other source will be dropped without further action; col. 7,

lines 25-29; if a trace_route packet is received, the packet is discarded; see also col. 10,

lines 27-32), and

       ii) in the absence of an adverse effect, allowing, by said test system, the

communication entities not having the adverse effect to communicate with said set of

machines *(col. 7, lines 39-43; another action can, of course, be to simply pass the packet*

through to its destination [targeted hosts/servers]; col. 10, lines 27-32; if the connection is

not allowed, it is blocked (box 970), but otherwise, it is allowed, and then the method tests

whether it is an initial connection (box 980) - if so, then at box 990 the connection is

established).

       Baehr discloses running said communication entities directed toward said test

system to detect possibly adverse effects on said test system, as recited above, but does not

explicitly discloses running said communication entities directed toward said test system

on said test facilities to detect possibly adverse effects on said test system.

       However, in an analogous art, Nakae discloses an attack defending

system/method including the steps of running said communication entities directed toward

said test system on said test facilities to detect possibly adverse effects on said test system

(Nakae: pars. 0126-0130; Figs. 7 and 10-11; steps A6-A8; the attack detecting section 202

of the decoy unit 2 compares the processing status notified from the processor 201 with a

normal operation definition to determine whether an attack exists; pars. 0153-0157; in the

decoy unit 2, the processor 201 provides WWW services to the attack-source host 301 and

sequentially notifies the attack detecting section 202 of the operation status such as file

accesses and network accesses).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the teaching of Nakae with the method and system

of Baehr to include the steps of running said communication entities directed toward said

test system on said test facilities to detect possibly adverse effects on said test system to

provide users with an attack defending system to lure suspicious packets into a decoy unit

to detect attacks and provide appropriate action to the detected attacks *(Nakae: pars. 0103-*

0104).

- **Regarding claim 38**, Baehr and Nakae disclose the method of claim 37.

Baehr further discloses said at least part of said communication entities directed

toward said test system include communication entities from traffic bound toward said set

of machines *(Baehr: col. 6, lines 29-36; Fig. 6; when a data packet arrives from the public*

network 350 addressed to one of the hosts or server 360-380; such packet typically include

a sources address, a destination address; see also col. 10, lines 11-18).

- **Regarding claim 39**, Baehr and Nakae disclose the method of claim 37.

    Baehr and Nakae further disclose said at least part of said communication entities directed toward said test system include communication entities from traffic coming from said set of machines *(Baehr: col. 8, lines 13-29; upon execution of such operations, a proxy host may then return a given packet to the sender, i.e. send the packet off with the original sender's address as the destination; that packet will then go through the screen 340, which will subject it to the predetermined inspection criteria, just as when it was first received at the screen from, for instance, public network 350; Nakae: pars. 0509-0512; Fig. 58; the present invention is further provided with a mirroring unit 6901, which copies the contents of a file system from the server (for example, an FTP server 402) on the internal network 4 to at least the decoy unit).*

- **Regarding claim 46**, Baehr and Nakae disclose the method of claim 37.

    Baehr and Nakae further disclose in the presence of said adverse effect, the step of subjecting to a resetting step those of said test facilities in said test system affected by said adverse effect *(Baehr: col. 6, lines 37-67 to col. 7, lines 1-7; packet is either blocked or allowed depending on predetermined criteria and/or predefined table; col. 7, lines 13-24; actions are taken on each data packet by the screening system 340, based upon the foregoing criteria and the particular security protocol and level for that packet as determined in advance by the system administrator; Nakae: pars. 0233-0234;the defense rule determination section 1001 instructs the confidence management sections 502 and 701 to reset a corresponding confidence level depending on an alert received from the decoy unit 2 through the control interface 106).*

- **Regarding claim 47**, Baehr and Nakae disclose the method of claim 37.

Baehr further discloses the machines in said set comprise facilities exposed to said adverse effect as well as additional contents, comprising the step of configuring said test facilities in order to replicate said facilities exposed to said adverse effect in the machines in said set *(Baehr: col. 4, lines 33-63; a proxy network may thus include proxy hosts representing actual hosts, and/or proxy hosts with unique servers, in any combination (zero to several of each); whichever configuration is adopted, the private network 330 and the proxy network 430 together form a single logical or apparent network 345, i.e. a single apparent domain from the point of view of outsiders; see also col. 7, lines 13-24).*

- **Regarding claim 48**, Baehr and Nakae disclose the method of claim 37.

Baehr further discloses inhibiting said test machines in said test system from providing responses to said traffic *(Baehr: col. 6, lines 53-59; in this case, the screen 340 should drop the packet without reply; col. 7, lines 16-24; packets from any other source will be dropped without further action; col. 7, lines 25-29; if a trace_route packet is received, the packet is discarded).*

- **Regarding claim 49**, Baehr and Nakae disclose the method of claim 37.

Baehr further discloses providing an in-line component ensuring said traffic with said set of machines *(Baehr: col. 3, lines 59-64; Figs. 5-9; packet screening system 340 and network interface 1)*; and

providing at least one interface interfacing said in-line component with said test

system *(Baehr: col. 3, lines 59-64; Figs. 5-9; packet screening system 340 and network*

interface 2).

- **Regarding claim 50**, Baehr and Nakae disclose the method of claim 49,

comprising the step of providing feedback from said test system to said in-line component

via said at least one interface *(Baehr: col. 8, lines 5-12; the screen can store information*

about what state each packet is in, and take actions dependent upon that state; see also col.

7, lines 55-63; packets will normally be logged in the log file storage 640 (especially failed

attempts or requests), including whatever information the system administrator decides is

important, such as: time of day; source and destination addresses; requested operation(s)).

- **Regarding claim 51**, Baehr and Nakae disclose the method of claim 49.

Baehr further discloses providing a management network for managing said test

system *(Baehr: col. 7, lines 13-24; administrator is able to select security protocol and*

predefined criteria for packet filtering/processing); and

providing feedback from said test system to said in-line component via said

management network *(Baehr: col. 7, lines 55-63; packets will normally be logged in the*

log file storage 640 (especially failed attempts or requests), including whatever

information the system administrator decides is important, such as: time of day; source and

destination addresses; requested operation(s); col. 8, lines 5-12; the screen can store

information about what state each packet is in, and take actions dependent upon that state).

- **Regarding claims 54-56**, claims 54-56 are similar in scope to claims 37-39 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 63-68**, claims 63-68 are similar in scope to claims 46-51 respectively, and are therefore rejected under similar rationale.

- **Regarding claim 71**, claim 71 is similar in scope to claim 54 and is therefore rejected under similar rationale.

- **Regarding claim 72**, claim 72 is similar in scope to claim 37 and is therefore rejected under similar rationale.

9.   **Claims 40-45, 52-53, 57-62, and 69-70 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Baehr in view of Nakae, as applied to claims 37 and 54 above, and further in view of Ramsey et al., (hereinafter "Ramsey"), U.S. Patent No. 7,331,061, filed on September 07, 2001.

- **Regarding claim 40**, Baehr and Nakae disclose the method of claim 37.

   Baehr and Nakae do not explicitly discloses providing a data base comprising patterns representative of forbidden communication entities for communication with said set of machines; and blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base.

   However, in an analogous art, Ramsey discloses an integrated computer security management method including steps of providing a data base comprising patterns representative of forbidden communication entities for communication with said set of

machines *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 18, lines 29-55; Fig. 5, wherein at least steps 542: signature match? Y/N and profile match: Y/N)*; and blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 17, lines 20-35; Fig. 5; wherein at least steps 514/528/652: deny/reject? Y/N)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Ramsey with the method and system of Baehr and Nakae to include steps of providing a data base comprising patterns representative of forbidden communication entities for communication with said set of machines; and blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base to provide user with a means for managing security information with parallel processing, serial processing, or singular processing by a firewall, and IDS, and an AVS *(Ramsey: col. 2, lines 63-67)*.

- **Regarding claim 41**, Baehr and Nakae disclose the method of claim 37.

Baehr and Nakae do not explicitly disclose providing a further data base comprising patterns representative of allowed communication entities for communication with said set of machines; and allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base.

However, in an analogous art, Ramsey discloses an integrated computer security management method including steps of providing a further data base comprising patterns

representative of allowed communication entities for communication with said set of

machines *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 18, lines*

29-55; Fig. 5, wherein at least steps 538: compare packet/copy to IDS signature and 542:

signature match? Y/N and profile match: Y/N); and allowing communication of allowed

communication entities in said traffic as identified by respective patterns included in said

further data base *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col.*

17, lines 20-35; Fig. 5; wherein at least steps : compare packet/copy to IDS signature;

552: trust? Y/N and 514/528/652: deny/reject? Y/N).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the teaching of Ramsey with the method and

system of Baehr and Nakae to include steps of providing a further data base comprising

patterns representative of allowed communication entities for communication with said set

of machines; and allowing communication of allowed communication entities in said

traffic as identified by respective patterns included in said further data base to provide user

with a means for managing security information with parallel processing, serial processing,

or singular processing by a firewall, and IDS, and an AVS *(Ramsey: col. 2, lines 63-67)*.

- **Regarding claim 42**, Baehr, Nakae, and Ramsey disclose the method of claim

40.

Baehr and Ramsey further disclose detecting unknown communication entities in

said traffic as identified by respective unknown patterns not included in said data base

(Baehr: col. 7, lines 13-29; packages from (or to) any other source (unknown source) will

be dropped; Ramsey: Fig. 5; wherein at least step 542: 'profile match? Y/N'); and

directing said unknown communication entities in said traffic as identified by respective

unknown patterns not included in said data base toward said test system to be run on said

test facilities to detect possibly adverse effects on said test system *(Baehr: col. 4, lines 57-*

60; Figs. 4-7; requests from public network will be forwarded to proxy network; see also

col. 6, lines 30-36; Ramsey: Fig. 5; wherein at least step 542: 'profile match? Y/N').

- **Regarding claim 43**, Baehr, Nakae, and Ramsey disclose the method of claim

42.

Baehr further discloses in the presence of said adverse effect, the step of adding

to said data base the respective pattern identifying the communication entity leading to said

adverse effect *(Baehr: col. 6, lines 37-59; col. 7, lines 55-63; packets, especially failed*

attempts or requests, are logged in the log file storage 640).

- **Regarding claim 44**, Baehr, Nakae, and Ramsey disclose the method of claim

41.

Baehr and Ramsey further disclose detecting unknown communication entities in

said traffic as identified by respective unknown patterns not included in said further data

base *(Baehr: col. 7, lines 13-29; unknown packets are determined by predetermined*

criteria; Ramsey: Fig. 5; wherein at least steps 512 and 552: determine if packet is

trusted? Y/N); and

directing said unknown communication entities in said traffic as identified by

respective unknown patterns not included in said further data base toward said test system

to be run on said test facilities to detect possibly adverse effects on said test system *(Baehr:*

col. 4, lines 57-60; Figs. 4-7; requests from public network will be forwarded to proxy

network; see also col. 6, lines 30-36).

- **Regarding claim 45**, Baehr, Nakae, and Ramsey disclose the method of claim 44.

Baehr and Ramsey further disclose in the absence of said adverse effect, the step of adding to said further data base the respective pattern identifying the communication entity failing to lead to said adverse effect *(Baehr: col. 7, lines 13-29; unknown packets are determined by predetermined criteria; Ramsey: col. 12, lines 63-67 to col. 13, lines 1-3; updating IDS configuration and/or signature files).*

- **Regarding claim 52**, Baehr, Nakae, and Ramsey disclose the method of claim 43.

Ramsey further discloses providing a parallel intrusion preventing arrangement including a respective data base including patterns representative of respective forbidden communication entities for communication with a respective set of machines *(Ramsey: col. 16, lines 23-30; parallel processing occurs where the IDS 255 processes the copied packet while the actual packet is processed by the firewall 225)*; and

in the presence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective data base, the respective pattern identifying the communication entity leading to said adverse effect *(Ramsey: col. 16, lines 23-60; decision step 512, it is determined whether a packet is 'trusted').*

- **Regarding claim 53**, Baehr, Nakae, and Ramsey disclose the method of claim 45.

Ramsey further discloses providing a parallel intrusion preventing arrangement including a respective further data base including patterns representative of respective allowed communication entities for communication with a respective set of machines *(Ramsey: col. 16, lines 23-30; col. 19, lines 8-34; parallel processing occurs where the IDS 255 processes the copied packet while the actual packet is processed by the firewall 225)*; and

in the absence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective further data base, the respective pattern identifying the communication entity failing to lead to said adverse effect *(Ramsey: col. 16, lines 23-60; col. 19, lines 8-34; decision step 512, it is determined whether a packet is 'trusted')*.

- **Regarding claims 57-62**, claims 57-62 are similar in scope to claims 40-45 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 69-70**, claims 69-70 are similar in scope to claims 52-53 respectively, and are therefore rejected under similar rationale.

Conclusion

10.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner

can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information

for unpublished applications is available through Private PAIR only. For more information

about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on

access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-

217-9197 (toll-free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-9199 (IN USA

OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437